SFA Modernization Partner

United States Department of Education
Student Financial Assistance

Single Sign-On Products Evaluation

RFI Response Review
Task Order #59

Version 1.0

August 31, 2001

Table of Contents

1. Introduction

In response to an SFA Request for Information (RFI) solicitation for a Single Sign-On (SSO) solution for the Schools Portal, software vendors provided Technical and Financial information. The RFI was based upon the authentication requirements for Schools Portal, NSLDS, RFMS, and DLOS. The companies and products that were evaluated included the following:

- IBM Tivoli – Policy Director
- Securant – Clear Trust
- Computer Associates – Single Sign-On
- BMC – Control-SA
- Netegrity – SiteMinder
- Entrust – GetAccess

Companies who did not respond included:

- Symantec
- OpenNetworks

This summary report describes the following:

- Evaluation Procedures
- Single Sign-On Functionality (with respect to SFA Requirements)
- Costing Options for VDC Operation and Maintenance
- Recommendations and Conclusions

Upon reviewing the RFI Responses, it was concluded that BMC did not offer a Single Sign-On product and was thus excluded from further evaluation.

2. Evaluation Procedures

Typical vendors response included the following material:

- SSO Technical Requirements
- SSO Costs and Qualifications
- Supplementary Documentation

The RFI responses were evaluated by the Modernization Partner team using the following criteria:

- Single Sign-On Technical Requirements Fulfillment
- SSO Hardware/Software Configuration Design
- VDC Rough Order of Magnitude (ROM) Operations Costing
- Phone Interviews with SSO technical and sales support staff

3. SFA Single Sign-On Technical Requirements Fulfillment

The RFI was based upon SFA requirements developed from US Government Standards, industry best practices and specifications from Schools Portal, DLOS, RFMS, and NSLDS. We then specified evaluation criteria for responses and rated the solutions for each section accordingly. The results of the evaluation are detailed in the Appendix A.

What was found during this exercise is that the technical Single Sign-On Solutions reviewed offered similar functionality and rated closely together. In ranking the products the defining factors became its integration capabilities with authentication databases, complexity of architecture, and scalability.

4. VDC Costing Options for SSO Operations and Maintenance

A 3-year estimate for the proposed vendor solutions was submitted by CSC as shown in the following table. These ROM costs were based on support of Schools Portal managed Single Sign-On accounts in a redundant, fail-over configuration as determined by vendor hardware specifications and software licensing fees.

	Users	YR 1	YR 2	YR3	Total
IBM	13000	$1.783M	1.468M	1.441M	$4.692 M
Entrust	13000	$1.482M	1.147M	1.126M	$3.755 M
Securant	13000	$803K	691K	679K	$2.173 M
Netegrity	13000	$780K	583K	573K	$1.936 M
CA	10000	$663K	663K	653K	$1.979M

The component software licensing costs (from the vendor RFI responses) are shown here. This itemization breakout has been included in the VDC ROM estimate.

	Users	YR 1	YR 2	YR3	Total
IBM	13000	$370K	74K	74K	$518K
Entrust	13000	$405K	71K	71K	$547K
Securant	13000	$170K	58K	58K	$286K
Netegrity	13000	$246K	49K	49K	$344K
CA	10000	$130K	130K	130K	$389K

5. Recommendations and Conclusions

The requirements for Single Sign-On (SSO) for Schools Portal have been based on several key assumptions:

- Financial Aid Professionals want to simplify the number of usernames and passwords required for access to SFA systems via the portal.
- There are no common authentication procedures available today among the applications connected with Schools Portal.
- Diverse databases provide key security features for identification, authentication, and access-control.
- SSO technology vendors have authentication software tools to solve these issues.

An assessment of the vendor RFI responses has produced a range of implementation strategies and costs, which can satisfy these security authentication needs. The Modernization Partner has made specific recommendations to meet these objectives:

1. The SFA IRB will receive a detailed Business Case describing an 8-month schedule for developing baseline Single Sign-On authentication services.

2. The Modernization Partner will develop an Authentication Framework which is reusable for future portal systems. This solution is not a 'throw-away' development effort.

3. Scalability requirements will be a determining factor in the vendor selection process. This issue impacts SFA strategic planning for VDC operations and maintenance costs, software licensing, and interoperabilty with the SFA Enterprise.

4. Centralized Security Management via Directory Services (LDAP) and data modelling of Schools Portals user accounts is required for any SSO vendor solution.

5. The high availability solution will include 7x24 maintenance and support, platform redundancy, and failover.

6. A RFP will be written to consolidate the findings of the SSO RFI process and the vendor response proposals.

7. The most viable solutions for the Schools Portal SSO initiative are IBM's Tivoli Policy Director and Netegrity's SiteMinder. IBM's Policy Director has the ability to integrate in SFA's IBM-centric environment. IBM's bundled directory server also provides a means for storing user credentials. Netegrity's strengths includes leadership in the Web Access Control market and the most flexible architecture interoperabilty with directories, portals, web server and mainframe security domains.

6. Solution #1: Netegrity's SiteMinder

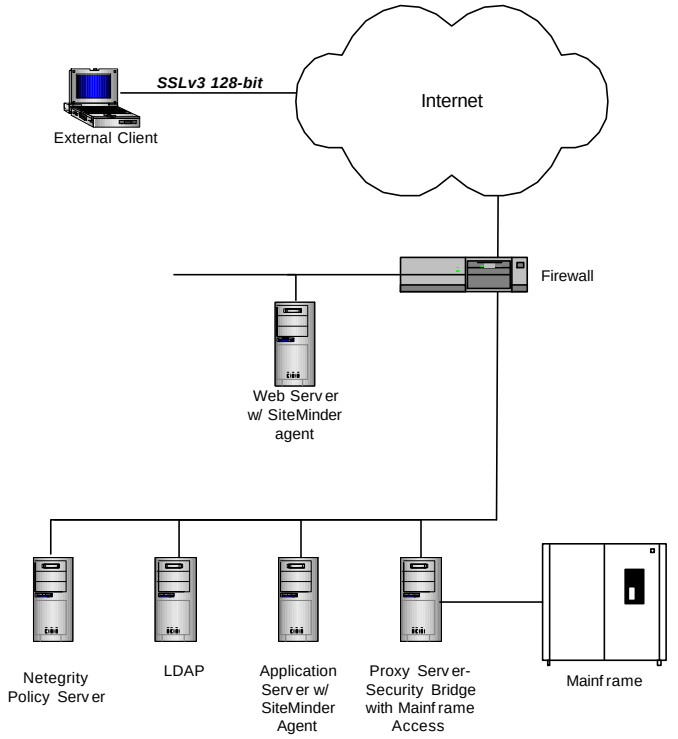
6.1 How it Works:

The Web Agent caches the successful authentication, and issues a SSO cookie to the user's browser. When the user accesses protected resources in other realms with the same protection level, they do not have to re-authenticate. Also, if the user moves to another Web server within this cookie domain, then the SSO cookie provides the appropriate session information to allow the user access, provided the protection level rules were maintained.

Further levels of access control will be handled either by the application or by integrating with a Directory Server.

6.2 Integration into the Existing Architecture

Netegrity supports the proposed architecture.



6.3 Requirements

- Runtime agent on supported Web Server
- One NT Policy Server
- Runtime agent on WebSphere with EJB security implemented

6.4 Advantages:

- Direct Integration with LDAP – no need for separate registry server
- High Scalability (based on independent test results)
- API for custom authentication types
- Flexible Architecture – Does not require a proprietary Authentication Directory.
- Has RACF integration through Security Bridge.

6.5 Disadvantages:

- Delegated Administration tools are a separate product.
- Highly dependant on cookies

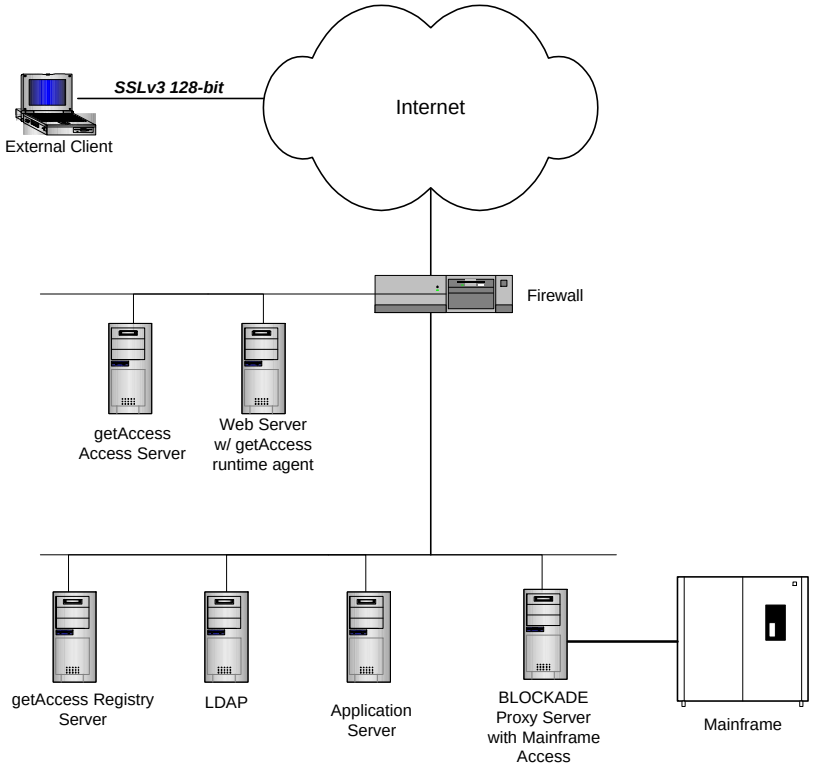
7. Solution #2: Entrust GetAccess

7.1 How It Works:

getAccess does two things to reduce the overhead associated with this repeated authentication and authorization. First, when a user is initially authenticated, their list of available resources is placed into their encrypted cookie. Second, the getAccess runtime agent loads a list of resources protected on the web server into memory. When a request comes in, the getAccess agent decrypts the cookie and compares the user's resource list with the resources loaded in memory. If there is a match, the resource is returned to the user. If not, the user is denied access.

7.2 Integration into the Existing Architecture

It is not stated in the RFI response that IBM HTTP Server and Websphere is supported.



7.3 Requirements:

- NT Access Server (located in DMZ).
- NT Registry Server (located in protected subnet)
- Runtime agent on web server

7.4 Advantages:

- Web-based administration tool
- Has Call Center Integration

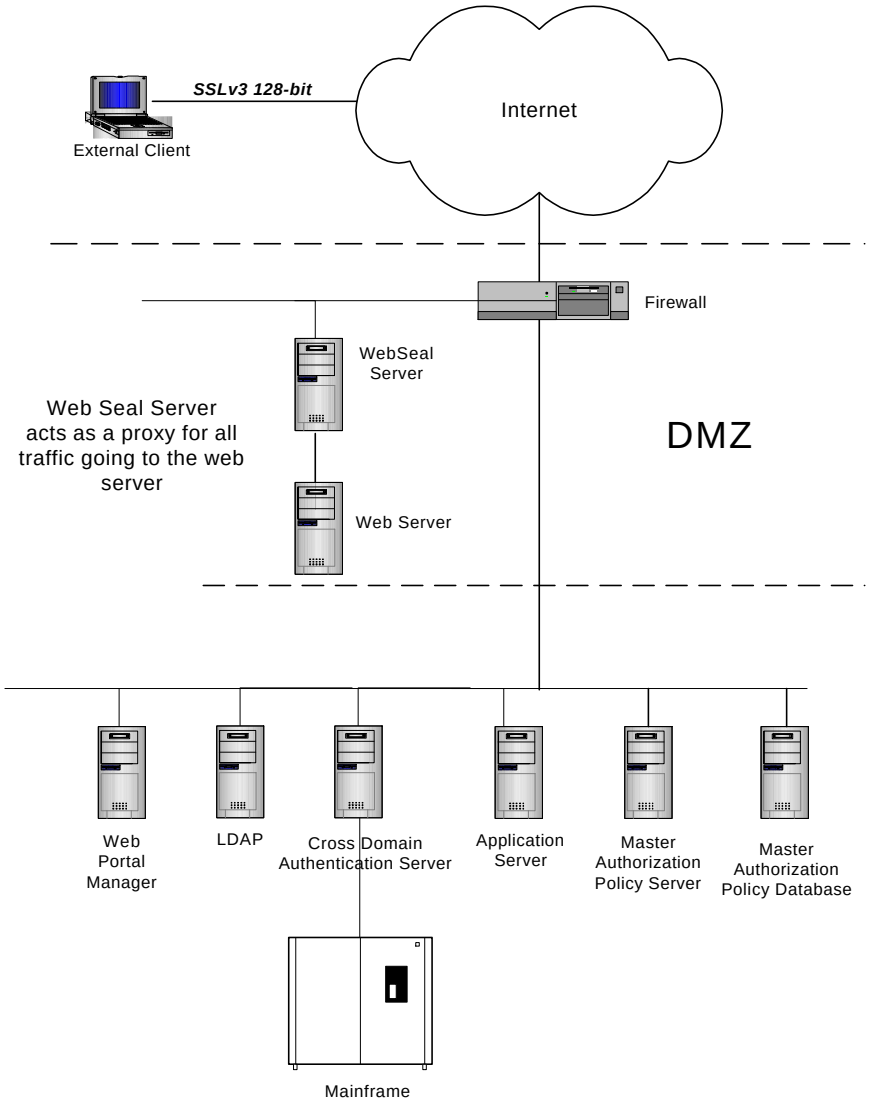
7.5 Disadvantages:

- No integration with RACF – Blockade is not a viable alternative for integration due to cost.
- GetAccess has schema constraints with LDAP directory servers
- Entirely cookie based.
- Have to use getAccess Administration GUI.

8. Solution #3 – IBM's Tivoli Policy Director

8.1 How it Works:

Policy Director uses a "Web Seal" server which acts as a proxy for any web server. Secure traffic will be routed to the Web Seal server first. The Web Seal server will prompt for username and password. Once entered, the Web Seal server checks the LDAP directory, and if it matches, allows access to the web server.



8.2 Integration into the Existing Architecture

Policy Director supports the proposed architecture.

8.3 Requirements

- Web Seal server running on AIX, NT, or Solaris
- 4 additional authorization and management servers

8.4 Advantages:

- Security for MQ-Series
- Java-based console
- Cookie only used for session management
- SecureWay LDAP bundled
- All policies stored in local cache for performance

8.5 Disadvantages:

- New Delegated Administration tool
- Session timeout is not configurable per user type
- Complex Architecture
- Infrastructure Intensive (Proxy Needed)
- Schemas are not customizable
- Scalability

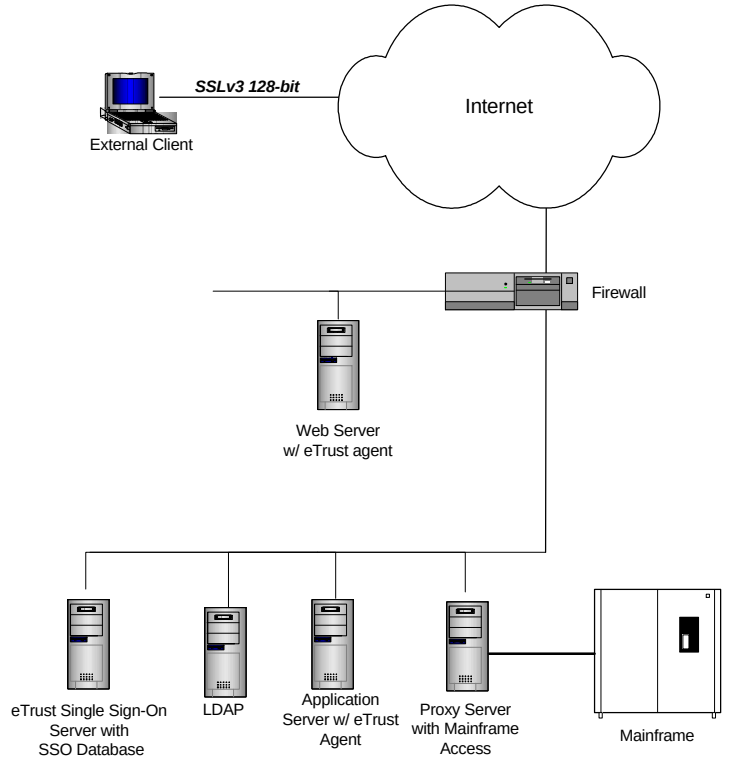
8.6 Misc. Notes:

- Authorization API included for Legacy Applications
- Authorizations (resources) defined in a proprietary database

9. Solution #4: Computer Associates Single Sign-On

9.1 How it Works:

CA Single Sign-On uses an SSO Database and login scripting to manage the authentication process. An eTrust agent on the Web Server intercepts a login request. If this is a first time login, authentication takes place on the eTrust SSO Server which grants or denies the request. Subsequent logins are validated by the WebServer eTrust agent. If the request is granted, the Web Agents sends a cookie, wrapped around an encrypted eTrust SSO ticket to the user browser. This ticket contains user identification data and a list of applications for which the user is authorized to access.



9.2 Integration into the Existing Architecture

CA eTrust SSO supports the proposed architecture.

9.3 Requirements

- Runtime agent on supported Web Server
- One NT or Unix Single Sign-On Server

9.4 Advantages:

- Works with Websphere Portal application builder
- Direct Integration with LDAP using eTrust Directory
- High Scalability (based on independent test results)
- API for custom authentication types

9.5 Disadvantages:

- Session cookies are stored on user hard disk for Web SSO login
- Authentication to unsupported applications implemented using 'Web Form Fill' scripting
- CA eTrust SSO Database is proprietary, 'black box' implementation

10. Solution #5: Securant ClearTrust Single Sign-On

10.1 How it Works:

Login to the Web Access server is monitored by a SecureControl plugin which forwards authentication requests to the Primary SecureControl Servers. The three Primary Control servers include Primary Authorization, Entitlement, and Authorization Dispatcher/Key Server. The Entitlements Database is the control center for the ClearTrust system where user, resource, and security policy is stored. Session cookies at the webserver plugin manage the SSO login.

10.2 Integration into the Existing Architecture

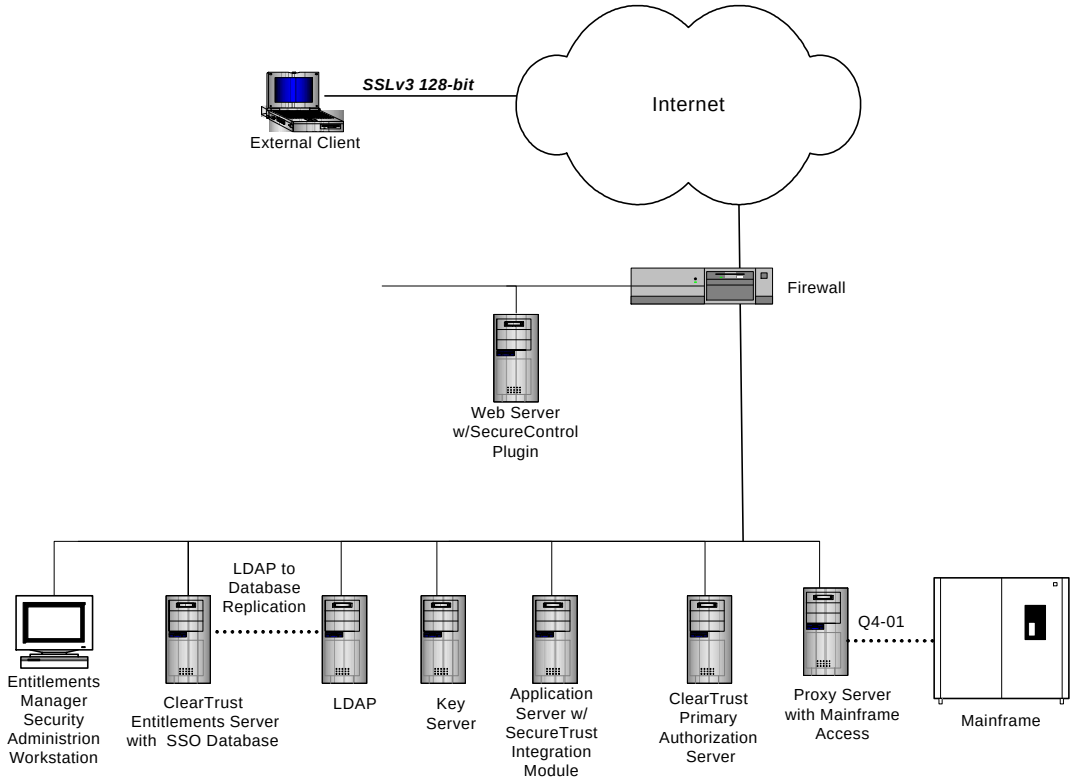
Securant ClearTrust SSO ***does not*** currently support the proposed architecture (RACF).

10.3 Requirements

- SecureControl Plugin on supported Web Server
- 3 NT or Unix Single Primary Control Servers

10.4 Advantages:

- LDAP Support with replication to Entitlements Database
- Entitlements Database (Oracle) not proprietary
- Session cookies are volatile (not stored)
- API for custom authentication types
- Interoperable with IBM HTTP Server 1.3.x and Websphere 3.5 on SUN SOLARIS platform



10.5 **Disadvantages:**

- Complex architecture (hardware intensive)
- RACF Integration in Beta (not costed)

APPENDIX A – SSO Evaluation Criteria Scoresheet

			Netegrity		Entrust		Securant		IBM		BMC		CA	
Cat. #	Criteria	Weight (1-5)	Score	W. Score	Score	W. Score	Score	W. Score	Score	W. Scor	Score	W. Score	Score	W. Scor
3.1	Company Information	5	4	0.217	4	0.217	4	0.217	5	0.27	5	0.272	5	0.27
3.2	Product Information	4	5	0.217	4	0.174	4	0.174	5	0.22	5	0.217	5	0.22
4.1	Access Control	5	5	0.272	5	0.272	4	0.217	4	0.22	2	0.109	4	0.22
4.2	Authentication	5	4	0.217	3	0.163	4	0.217	5	0.27	5	0.272	5	0.27
4.3	Password Policy	4	4	0.174	5	0.217	5	0.217	4	0.17	4	0.174	5	0.22
4.4	Audit	4	5	0.217	5	0.217	4	0.174	5	0.22	4	0.174	4	0.17
4.5	Client Management / Access	4	4	0.174	5	0.217	5	0.217	4	0.17	2	0.087	4	0.17
4.6	Applications	5	5	0.272	5	0.272	5	0.272	4	0.22	5	0.272	4	0.22
4.7	Multi-site, Multi-domain and Third Party Support	5	5	0.272	5	0.272	5	0.272	5	0.27	0	0	5	0.27
4.8	Session Management	4	4	0.174	4	0.174	4	0.174	4	0.17	2	0.087	3	0.13
4.9	Web Servers	3	5	0.163	5	0.163	5	0.163	5	0.16	2	0.065	5	0.16
4.10	Portal Platforms	4	4	0.174	4	0.174	4	0.174	4	0.17	3	0.13	4	0.17
4.11	Directory Support	4	5	0.217	4	0.174	4	0.174	3	0.13	2	0.087	5	0.22
4.12	PKI Support	3	5	0.163	5	0.163	5	0.163	5	0.16	2	0.065	5	0.16
4.13	Architecture Overview	5	5	0.272	4	0.217	4	0.217	3	0.16	5	0.272	4	0.22
4.14	Platforms Support	3	5	0.163	5	0.163	5	0.163	5	0.16	5	0.163	5	0.16
4.15	APIs and SDKs	5	5	0.272	5	0.272	5	0.272	5	0.27	5	0.272	5	0.27
4.16	Standards Compliance	3	5	0.163	5	0.163	5	0.163	5	0.16	5	0.163	5	0.16
4.17	Performance, Scalability, High-Availability	4	5	0.217	4	0.174	3	0.13	3	0.13	5	0.217	4	0.17
5.0	Operations	4	5	0.217	5	0.217	4	0.174	4	0.17	5	0.217	5	0.22
6.0	Administration	5	4	0.217	4	0.217	5	0.272	4	0.22	4	0.217	4	0.22
7.1	Documentation	2	5	0.109	5	0.109	5	0.109	5	0.11	5	0.109	5	0.11
7.2	Training	2	5	0.109	5	0.109	5	0.109	5	0.11	5	0.109	5	0.11
	Total Score			***4.663***		***4.511***		***4.435***		***4.337***		***3.750***		***4.522***